

JP2002259344 A

ONE-TIME PASSWORD AUTHENTICATION SYSTEM, PORTABLE
TELEPHONE AND USER IDENTIFICATION SERVER

MITSUBISHI ELECTRIC CORP

Inventor(s):YONEDA TAKESHI

Application No. 2001053911 JP2001053911 JP, Filed 20010228,A1 Published
20020913Published 20020913

Abstract: PROBLEM TO BE SOLVED: To easily manage secret information while securing the safety of a one-time password concerning user authentication using the one-time password in an information communication network system.

SOLUTION: A hush generation part 113 in a portable telephone set 101 obtains a hush value by using a user ID, present time information and common secret information and generates the one-time password. In a user authentication server 103 receiving the user ID and the one-time password from a user PC 102, a hush generation part 124 generates the one-time password similarly by using the received user ID, the present time information and the common secret information to use it for verification by a one-time password verification part.

Int'l Class: G06F01500; H04B00726 H04Q00738 H04L00932 H04Q00734

Patents Citing this One: No US, EP, or WO patents/search reports have cited this patent. MicroPatent Reference Number: 000618317

COPYRIGHT: (C) 2002JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-259344
(P2002-259344A)

(43) 公開日 平成14年9月13日 (2002.9.13)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
H 0 4 B 7/26		H 0 4 B 7/26	M 5 J 1 0 4
H 0 4 Q 7/38			1 0 9 S 5 K 0 6 7
H 0 4 L 9/32			1 0 9 M
H 0 4 Q 7/34		H 0 4 L 9/00	6 7 3 C

審査請求 未請求 請求項の数 8 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願2001-53911(P2001-53911)

(22) 出願日 平成13年2月28日 (2001.2.28)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 米田 健

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100099461

弁理士 溝井 章司 (外2名)

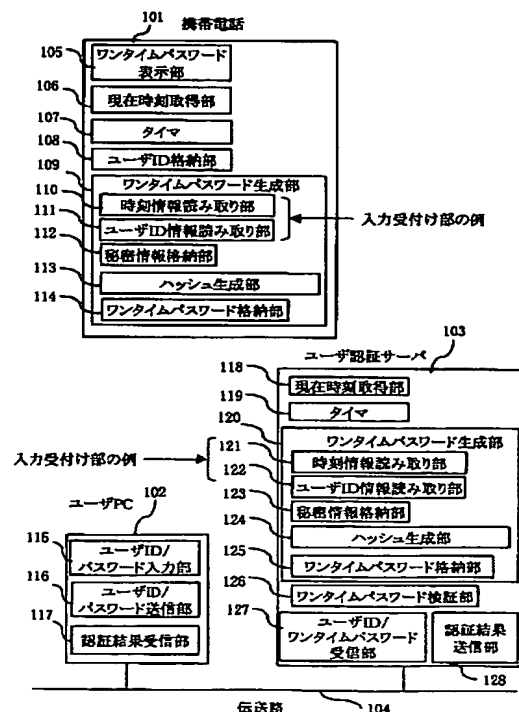
最終頁に続く

(54) 【発明の名称】 ワンタイムパスワード認証システム及び携帯電話及びユーザ認証サーバ

(57) 【要約】

【課題】 情報通信ネットワークシステムにおけるワンタイムパスワードを利用したユーザ認証に係り、ワンタイムパスワードの安全性を担保しつつ、秘密情報の管理を容易にすることを課題とする。

【解決手段】 携帯電話101のハッシュ生成部113で、ユーザIDと、現在時刻情報と、共通の秘密情報とを用いて、ハッシュ値を求め、ワンタイムパスワードを生成する。ユーザPC102からユーザIDとワンタイムパスワードを受信したユーザ認証サーバ103は、ハッシュ生成部124で、受信したユーザIDと、現在時刻情報と、共通の秘密情報とを用いて、同様にワンタイムパスワードを生成し、ワンタイムパスワード検証部による検証に用いる。



【特許請求の範囲】

【請求項 1】 ユーザ端末に接続するユーザ認証サーバと、携帯電話とからなるワнтаイムパスワード認証システムであって、

携帯電話は、（１）秘密情報を格納する携帯電話側秘密情報格納部と、（２）ユーザＩＤと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワнтаイムパスワードを生成する携帯電話側ハッシュ生成部と、（３）生成したワнтаイムパスワードを表示するワнтаイムパスワード表示部とを有し、

ユーザ認証サーバは、（４）ユーザＩＤとワнтаイムパスワードとを、ユーザ端末から受信するユーザＩＤ／ワнтаイムパスワード受信部と、（５）携帯電話側秘密情報格納部で格納する秘密情報と同一の秘密情報を格納するサーバ側秘密情報格納部と、（６）受信したユーザＩＤと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワнтаイムパスワードを生成するサーバ側ハッシュ生成部と、（７）サーバ側ハッシュ生成部で生成したワнтаイムパスワードと、ユーザＩＤ／ワнтаイムパスワード受信部で受信したワнтаイムパスワードとを比較し、一致した場合に認証結果を成功とするワнтаイムパスワード検証部と、

（８）認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とするワнтаイムパスワード認証システム。

【請求項 2】 上記携帯電話側ハッシュ生成部は、携帯電話側秘密情報格納部に格納する秘密情報を鍵として共通鍵暗号方式により、現在時刻情報と、ユーザＩＤとの MAC (Message Authentication Code) を生成し、その MAC をワнтаイムパスワードとし、

上記サーバ側ハッシュ生成部は、サーバ側秘密情報格納部に格納する秘密情報を鍵として共通鍵暗号方式により、現在時刻情報と、ユーザＩＤとの MAC を生成し、その MAC をワнтаイムパスワードとすることを特徴とする請求項 1 記載のワнтаイムパスワード認証システム。

【請求項 3】 上記携帯電話は、ユーザＩＤと現在時刻情報との入力を受け付ける携帯電話側入力受け部と、上記携帯電話側秘密情報格納部と、上記携帯電話側ハッシュ生成部とを含む携帯電話側ワнтаイムパスワード生成部を有し、

上記携帯電話側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワнтаイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有し、

上記ユーザ認証サーバは、ユーザＩＤと現在時刻情報と

の入力を受け付けるサーバ側入力受け部と、上記サーバ側秘密情報格納部と、上記サーバ側ハッシュ生成部とを含むサーバ側ワнтаイムパスワード生成部を有し、上記サーバ側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後はサーバ側ワнтаイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有することを特徴とする請求項 1 記載のワнтаイムパスワード認証システム。

【請求項 4】 上記携帯電話は、現在時刻情報の入力を受け付ける携帯電話側入力受け部と、上記携帯電話側秘密情報格納部と、ユーザＩＤを格納するユーザＩＤ格納部と、上記携帯電話側ハッシュ生成部とを含む携帯電話側ワнтаイムパスワード生成部を有し、

上記携帯電話側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワнтаイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有し、

上記ユーザＩＤ格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワнтаイムパスワード生成部の外部から読み出しが可能で、かつ書き込みが不可能である構成を有し、

上記ユーザ認証サーバは、ユーザＩＤと現在時刻情報との入力を受け付けるサーバ側入力受け部と、上記サーバ側秘密情報格納部と、上記サーバ側ハッシュ生成部とを含むサーバ側ワнтаイムパスワード生成部を有し、

上記サーバ側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後はサーバ側ワнтаイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有することを特徴とする請求項 1 記載のワнтаイムパスワード認証システム。

【請求項 5】 上記携帯電話側ワнтаイムパスワード生成部は、携帯電話に着脱可能な IC カードにより構成され、

IC カードが携帯電話に装着されることにより、携帯電話側ハッシュ生成部が、ワнтаイムパスワードを生成し、更に、ワнтаイムパスワード表示部が、ワнтаイムパスワードを表示することを特徴とする請求項 4 記載のワнтаイムパスワード認証システム。

【請求項 6】 携帯電話は、デジタル署名が付加された現在時刻情報を受信し、受信した現在時刻情報を検証する携帯電話側現在時刻取得部を有し、検証が成功した現在時刻情報により時刻調整する携帯電話側タイマとを有し、

携帯電話側ハッシュ生成部は、時刻調整された携帯電話側タイマが示す現在時刻情報を用い、

ユーザ認証サーバは、デジタル署名が付加された現在時刻情報を受信し、受信した現在時刻情報を検証するサーバ側現在時刻取得部を有し、

検証が成功した現在時刻情報により時刻調整するサーバ側タイマとを有し、

携帯電話側ハッシュ生成部は、時刻調整されたサーバ側タイマが示す現在時刻情報を用いることを特徴とする請求項1記載のワンタイムパスワード認証システム。

【請求項7】 ワンタイムパスワード認証システムを構成する携帯電話であって、(1) 秘密情報を格納する携帯電話側秘密情報格納部と、(2) ユーザIDと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成する携帯電話側ハッシュ生成部と、(3) 生成したワンタイムパスワードを表示するワンタイムパスワード表示部とを有することを特徴とする携帯電話。

【請求項8】 ユーザ端末に接続し、ワンタイムパスワード認証システムを構成するユーザ認証サーバであって、(1) ユーザIDとワンタイムパスワードとを、ユーザ端末から受信するユーザID/ワンタイムパスワード受信部と、(2) 秘密情報を格納するサーバ側秘密情報格納部と、(3) 受信したユーザIDと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成するサーバ側ハッシュ生成部と、(4) サーバ側ハッシュ生成部で生成したワンタイムパスワードと、ユーザID/ワンタイムパスワード受信部で受信したワンタイムパスワードとを比較し、一致した場合に認証結果を成功とするワンタイムパスワード検証部と、(5) 認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とするユーザ認証サーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、情報通信ネットワークシステムにおけるユーザ認証システムに関するものである。

【0002】

【従来の技術】 ワンタイムパスワード方式とは、利用者が頭で覚えているパスワードのかわりに、トークンと呼ばれる小さな携帯装置に表示されるパスワードを入力してユーザ認証を行う方式である(“Firewall and Internet Security”, William R. Cheswick, pp. 120)。図10は、トークンの外観を示す図である。図11は、従来のワンタイムパスワード認証システムの概要を示す図である。

【0003】 図12は、秘密情報の管理状態を示す図である。図に示すように、ユーザ毎にトークンを配布する必要がある。また、各トークンには、異なる秘密情報が格納され、その秘密情報は、ユーザ認証サーバのユーザID/秘密情報格納テーブルに登録される必要がある。

【0004】 図13は、従来技術におけるワンタイムパスワード認証システムの構成を示す図である。図14

は、従来技術におけるワンタイムパスワード認証システムの処理フローを示す図である。続いて処理について説明する。まず、トークン1301では、タイマ1305から時刻情報を取得する(ステップS1701)。次にワンタイムパスワード生成部1307において、時刻情報と秘密情報格納部1306に格納されている秘密情報とからハッシュ関数等の一方方向性関数を用いてワンタイムパスワードを生成する(ステップS1702)。生成されたワンタイムパスワードは、ワンタイムパスワード表示部1308に表示される(ステップS1703)。

【0005】 PCのユーザは、ユーザPC1302で起動しているアプリケーションのユーザID/パスワード入力部1309に、ユーザIDとワンタイムパスワードを入力する(ステップS1704)。入力されたユーザIDとワンタイムパスワードは、ユーザID/ワンタイムパスワード送信部1310より、ユーザ認証サーバ1303に伝送路1304経由で送信される(ステップS1705)。

【0006】 ユーザ認証サーバ1303は、ユーザIDとワンタイムパスワードを、ユーザID/ワンタイムパスワード受信部1312で受信すると(ステップS1706)、まず受け取ったユーザIDに対応する秘密情報をユーザID/秘密情報格納テーブル1316から選択し(ステップS1707)、タイマ1317から時刻情報を取得した後(ステップS1708)、ワンタイムパスワード生成部1313にて、時刻情報と秘密情報からワンタイムパスワードを生成する(ステップS1709)。ステップS1709にて生成されたワンタイムパスワードは、ワンタイムパスワード検証部1314において、受信したワンタイムパスワードと比較される(ステップS1710)。比較結果が一致すればユーザ認証成功であり、一致しなければ、失敗である。ユーザ認証サーバ1303は、ユーザ認証結果を認証結果送信部1315より、ユーザPC1302に伝送路1304経由で送信する(ステップS1711)。

【0007】 ユーザPC1312では、認証結果を認証結果受信部1311にて受信する(ステップS1712)。認証結果が成功であれば、業務処理を実行し(ステップS1714)、失敗であれば処理を終了する(ステップS1715)。

【0008】 クライアントサーバ方式を採用している情報通信システムにおいては、指紋やデジタル署名などの新しいユーザ認証方式を導入するためには、クライアントプログラムの大きな変更が必要である。一方トークンを用いたワンタイムパスワード方式では、クライアントプログラムで、ユーザ名とパスワードの入力を受け付ける際に、従来ユーザが頭で覚えているパスワードのかわりに、トークンに表示されるワンタイムパスワードが入力される。その違いをクライアントプログラムは区別する必要がない。したがって、クライアントプログラムの

変更が不要であるという長所がある。

【0009】

【発明が解決しようとする課題】従来の方式においては、ワンタイムパスワード生成・表示装置（トークン）を携帯しなければならない。しかし、社内電話のPHS化、携帯電話の普及が進み、一人一台携帯電話を持つ環境において、更にトークンを携帯することは、煩わしい。

【0010】また、従来の方式では、トークン毎に異なる秘密情報が必要であり、それらの秘密情報はすべてユーザ認証サーバに登録する必要があった。各秘密情報は、生成、登録の過程で機密に保護される必要がある。秘密情報の生成、登録作業はユーザの人数分実施する必要があり、その作業の間、秘密情報を機密に保つ手間は大きかった。上述の欠点を除くことを課題とする。

【0011】

【課題を解決するための手段】本発明に係るワンタイムパスワード認証システムは、ユーザ端末に接続するユーザ認証サーバと、携帯電話とからなるワンタイムパスワード認証システムであって、携帯電話は、（１）秘密情報を格納する携帯電話側秘密情報格納部と、（２）ユーザIDと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成する携帯電話側ハッシュ生成部と、（３）生成したワンタイムパスワードを表示するワンタイムパスワード表示部とを有し、ユーザ認証サーバは、（４）ユーザIDとワンタイムパスワードとを、ユーザ端末から受信するユーザID／ワンタイムパスワード受信部と、（５）携帯電話側秘密情報格納部で格納する秘密情報と同一の秘密情報を格納するサーバ側秘密情報格納部と、（６）受信したユーザIDと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成するサーバ側ハッシュ生成部と、（７）サーバ側ハッシュ生成部で生成したワンタイムパスワードと、ユーザID／ワンタイムパスワード受信部で受信したワンタイムパスワードとを比較し、一致した場合に認証結果を成功とするワンタイムパスワード検証部と、（８）認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とする。

【0012】上記携帯電話側ハッシュ生成部は、携帯電話側秘密情報格納部に格納する秘密情報を鍵として共通鍵暗号方式により、現在時刻情報と、ユーザIDとのMAC（Message Authentication Code）を生成し、そのMACをワンタイムパスワードとし、上記サーバ側ハッシュ生成部は、サーバ側秘密情報格納部に格納する秘密情報を鍵として共通鍵暗号方式により、現在時刻情報と、ユーザIDとのMACを

生成し、そのMACをワンタイムパスワードとすることを特徴とする。

【0013】上記携帯電話は、ユーザIDと現在時刻情報との入力を受け付ける携帯電話側入力受け部と、上記携帯電話側秘密情報格納部と、上記携帯電話側ハッシュ生成部とを含む携帯電話側ワンタイムパスワード生成部を有し、上記携帯電話側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有し、上記ユーザ認証サーバは、ユーザIDと現在時刻情報との入力を受け付けるサーバ側入力受け部と、上記サーバ側秘密情報格納部と、上記サーバ側ハッシュ生成部とを含むサーバ側ワンタイムパスワード生成部を有し、上記サーバ側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後はサーバ側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有することを特徴とする。

【0014】上記携帯電話は、現在時刻情報の入力を受け付ける携帯電話側入力受け部と、上記携帯電話側秘密情報格納部と、ユーザIDを格納するユーザID格納部と、上記携帯電話側ハッシュ生成部とを含む携帯電話側ワンタイムパスワード生成部を有し、上記携帯電話側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有し、上記ユーザID格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部から読み出しが可能で、かつ書き込みが不可能である構成を有し、上記ユーザ認証サーバは、ユーザIDと現在時刻情報との入力を受け付けるサーバ側入力受け部と、上記サーバ側秘密情報格納部と、上記サーバ側ハッシュ生成部とを含むサーバ側ワンタイムパスワード生成部を有し、上記サーバ側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後はサーバ側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有することを特徴とする。

【0015】上記携帯電話側ワンタイムパスワード生成部は、携帯電話に着脱可能なICカードにより構成され、ICカードが携帯電話に装着されることにより、携帯電話側ハッシュ生成部が、ワンタイムパスワードを生成し、更に、ワンタイムパスワード表示部が、ワンタイムパスワードを表示することを特徴とする。

【0016】携帯電話は、デジタル署名が付加された現在時刻情報を受信し、受信した現在時刻情報を検証する携帯電話側現在時刻取得部を有し、検証が成功した現在時刻情報により時刻調整する携帯電話側タイマとを有し、携帯電話側ハッシュ生成部は、時刻調整された携帯電話側タイマが示す現在時刻情報を用い、ユーザ認証サ

サーバは、デジタル署名が付加された現在時刻情報を受信し、受信した現在時刻情報を検証するサーバ側現在時刻取得部を有し、検証が成功した現在時刻情報により時刻調整するサーバ側タイマとを有し、携帯電話側ハッシュ生成部は、時刻調整されたサーバ側タイマが示す現在時刻情報を用いることを特徴とする。

【0017】本発明に係る携帯電話は、ワンタイムパスワード認証システムを構成する携帯電話であって、

(1) 秘密情報を格納する携帯電話側秘密情報格納部と、(2) ユーザIDと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成する携帯電話側ハッシュ生成部と、(3) 生成したワンタイムパスワードを表示するワンタイムパスワード表示部とを有することを特徴とする。

【0018】本発明に係るユーザ認証サーバは、ユーザ端末に接続し、ワンタイムパスワード認証システムを構成するユーザ認証サーバであって、(1) ユーザIDとワンタイムパスワードとを、ユーザ端末から受信するユーザID/ワンタイムパスワード受信部と、(2) 秘密情報を格納するサーバ側秘密情報格納部と、(3) 受信したユーザIDと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成するサーバ側ハッシュ生成部と、(4) サーバ側ハッシュ生成部で生成したワンタイムパスワードと、ユーザID/ワンタイムパスワード受信部で受信したワンタイムパスワードとを比較し、一致した場合に認証結果を成功とするワンタイムパスワード検証部と、(5) 認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とする。

【0019】

ハッシュ値 = Hash (ユーザID || 時刻情報 || 秘密情報) 式1

ユーザIDと時刻情報と秘密情報の間の記号は、結合を示している。Hash (X) は、情報XのHash値を生成することを示す。つまり、上式はユーザID、時刻情報、秘密情報をすべて結合し、その結合した情報からSHA1ハッシュアルゴリズムに従い、ハッシュ値を計算する。生成された20Byteのバイナリハッシュ値を、Base64により28文字のキーボード入力可能文字列に変換し、その先頭8文字をワンタイムパスワード表示部105に表示する(ステップS302)。なお、ハッシュ値の生成方法としてMAC(Message Authentication Code)を用いることも可能である。その場合、秘密情報をMISTYやDESなどの共通鍵暗号方式の鍵とする。そして、ユーザIDと時刻情報の結合情報から、上記鍵を利用して、MACを生成する。このMACをハッシュ値として利用する。

【発明の実施の形態】実施の形態1. 本実施の形態では、携帯電話、認証サーバに共通かつ唯一の秘密情報を格納する。つまり、ユーザ認証システムに用いられるすべての携帯電話と、認証サーバが単一の秘密情報を共有する。そして、携帯電話、認証サーバの時刻を同期させ、ユーザIDと時刻情報と秘密情報からワンタイムパスワードを生成する。ワンタイムパスワード生成部は、秘密情報格納部と、入力受付部と、ハッシュ生成部と、ハッシュ格納部を有している。秘密情報格納部は、一度だけ書き込みが可能で、以降外部からの読み出し、書き込みが不可であり、入力受付部は、外部から2つの入力のみを受け付け、ハッシュ生成部は、2つの入力と秘密情報格納部に格納された秘密情報とからハッシュ値を生成する。ハッシュ格納部は、そのハッシュを読み出し可能なように格納する。

【0020】図1は、実施の形態1におけるユーザ認証システムの構成を示す図である。図2は、実施の形態1におけるユーザ認証システムの概要を示す図である。図3は、実施の形態1におけるユーザ認証システムの処理フローを示す図である。まず、携帯電話101では、ワンタイムパスワードを生成する(ステップS301)。

【0021】図4は、ワンタイムパスワード生成の詳細フローを示す図である。まず、タイマ107から時刻情報を取得する(ステップS401)。時刻情報は現在時刻を分単位で表現したものである。次に、ユーザID格納部108に格納されているユーザIDを取得する(ステップS402)。ハッシュ生成部113において、ステップS401で取得した時刻情報と、ステップS402で取得したユーザIDと、秘密情報格納部112に格納されている秘密情報とからハッシュ関数等の一方向性関数を用いてワンタイムパスワードを生成する(ステップS403)。具体的な生成式を以下に示す。

【0022】PCのユーザは、ユーザPC102で起動しているアプリケーションのユーザID/パスワード入力部115に、ユーザIDとワンタイムパスワードを入力する(ステップS303)。入力されたユーザIDとワンタイムパスワードは、ユーザID/ワンタイムパスワード送信部116より、ユーザ認証サーバ103に伝送路104経由で送信される(ステップS304)。

【0023】ユーザ認証サーバ103は、ユーザIDとワンタイムパスワードを、ユーザID/タイムパスワード受信部127で受信すると(ステップS305)、ワンタイムパスワードを生成する(ステップS306)。図4に示すように、タイマ119から時刻情報を取得した後(ステップS401)、受信したユーザIDをユーザID情報読み取り部で読み取り、秘密情報格納部123から秘密情報を取得する。そして、ハッシュ生成部124で、時刻情報と、ユーザIDと、秘密情報時刻情報

と秘密情報とから上式によりハッシュ値を計算し、生成された20Byteのバイナリハッシュ値を、Base64により28文字のキーボード入力可能文字列に変換し、その先頭8文字をワнтаイムパスワードとする(ステップS403)。ステップS403にて生成されたワнтаイムパスワードは、ワнтаイムパスワード格納部125に格納される。

【0024】ワнтаイムパスワード検証部126は、ワнтаイムパスワード格納部125からワнтаイムパスワードを取得すると、受信したワнтаイムパスワードと比較する(ステップS307)。比較結果が一致すればユーザ認証成功であり、一致しなければ、時刻情報を一分前のものとし、ワнтаイムパスワードを計算し直す。その結果と一致すればユーザ認証成功であり、それでも一致しない場合は失敗とする。ユーザ認証サーバ103は、ユーザ認証結果を認証結果送信部128より、ユーザPC102に伝送路104経由で送信する(ステップS309)。

【0025】ユーザPC102では、認証結果を認証結果受信部117にて受信する(ステップS310)。認証結果が成功であれば、業務処理を実行し(ステップS312)、失敗であれば処理を終了する(ステップS313)。

【0026】上述のように、ワнтаイムパスワード生成部109、120は同一構成を有する。一度だけ書き込みが可能で、書き込み後は、外部からの読み出し、書き込みが不可である秘密情報格納部121と、外部から時刻情報の入力を受け付ける時刻情報読み取り部110、121と外部からユーザID情報の入力を受け付けるユーザID情報読み取り部と、時刻情報、ユーザID、秘密情報からハッシュを生成するハッシュ生成部113、124と外部から唯一読み出し可能な情報を格納するワнтаイムパスワード格納部とを含んでいる。

【0027】また、タイマ117、119は同期させる。現在時刻情報は、NHKの時報情報や、電波によるデジタル時刻情報配信サービスがあるため、それらの時刻情報を1日一回現在時刻取得部で受信し、タイマの時刻のずれを修正する。ユーザ認証サーバは、情報通信ネットワークに接続されているので、情報通信ネットワーク経由のNTP(Network Time Protocol)等の時刻同期機能によりタイマのずれを修正してもよい。

【0028】本実施の形態による効果について説明する。まず、携帯電話に表示されるワнтаイムパスワードは、ユーザID、時刻情報、秘密情報のハッシュ値であるので、ユーザIDと時刻情報のいずれかが異なればワнтаイムパスワードは異なる値となる。また、ユーザ認証サーバでは、ユーザID、時刻情報、秘密情報から同一のハッシュ値を再現できる。また、秘密情報は、ユーザの携帯電話、ユーザ認証サーバで共通のものを使って

いるが、外部からの読み出しが困難なワнтаイムパスワード生成部により機密に保たれている。したがって、第三者が他人のワнтаイムパスワードを推定することは困難である。したがって、本実施の形態で利用するワнтаイムパスワードは安全性が確保されている。

【0029】また、本実施の形態では、携帯される携帯電話にワнтаイムパスワードが表示されるため、新たにワнтаイムパスワード生成表示用のトークンを携帯する必要がない。そして、機密に保持する必要があるデータは、共通に利用される秘密情報のみであり、ユーザ認証サーバに、一度この秘密情報を登録すれば、ユーザ数が増加しても新たに登録する秘密情報はない。

【0030】実施の形態2。図5は、実施の形態2におけるワнтаイムパスワード生成部の構成を示す図である。本実施の形態では、携帯電話で利用するワнтаイムパスワード生成部として、一度だけ書き込みが可能で、書き込み後外部からの読み出し、書き込みが不可の秘密情報格納部506と、一度だけ書き込みが可能で、書き込み後外部から読み出しは可能であるが、書き込みは不可であるユーザID格納部503と、唯一の外部からの入力情報として時刻情報を受け付ける時刻情報読み取り部502、および実施の形態1におけるハッシュ生成部113、124と同一のハッシュ生成部504、ワнтаイムパスワード格納部505から構成されるワнтаイムパスワード生成部501を利用する。実施の形態1と異なるのは、ワнтаイムパスワード生成部において、ユーザID情報を外部から読み取るのではなく、ワнтаイムパスワード生成部の内部に、読み取り可、変更不可の状態に格納されたユーザID情報を利用する点である。

【0031】本実施の形態の効果について説明する。悪意のある者が、携帯電話を不正に分解し、ワнтаイムパスワード生成部を入手しても、外部からワнтаイムパスワード生成部に入力できる情報は、時刻情報に限られている。したがって、任意のユーザIDに対応する将来の時刻のワнтаイムパスワードを不正に入手することは困難となり、携帯電話の不正分解に対して、より安全なワнтаイムパスワード認証システムを構築することができる。

【0032】実施の形態3。ここでは、図5のワнтаイムパスワード生成部をICカードに持たせ、携帯電話にICカードを差し込むと携帯電話のディスプレイにワнтаイムパスワードが表示される形態について説明する。図6は、実施の形態3における携帯電話とICカードの構成を示す図である。ワнтаイムパスワード表示部602、現在時刻取得部603、タイマ604は図1における前述の105、106、107の要素と同一の機能を有する。ICカード挿入部605は、物理的なICカード差込口と、ICカードとの情報交換のインターフェースを提供する。ICカード606は、時刻情報読み取り部607、ユーザID格納部608、ワнтаイムパスワ

ード生成部609、ワнтаイムパスワード610、秘密情報格納部611から構成され、それぞれ、前述の502、503、504、505、506の要素と同一の機能を有する。

【0033】ワнтаイムパスワード生成の処理において、タイマ604の時刻情報は、時刻情報読み取り部607により読み取られ、それぞれユーザID格納部608と秘密情報格納部611に格納されているユーザID情報と秘密情報とともに、ハッシュ生成部609におけるハッシュ生成に用いられる。生成されたハッシュ値は、ワнтаイムパスワード格納部610にワнтаイムパスワードとして格納され、ICカード挿入部605を通してワнтаイムパスワード表示部602に表示される。

【0034】本実施の形態の効果について説明する。例えば、A社の提供するオンラインショッピングシステムと、B社の提供するオンラインバンキングシステムでユーザ認証が必要となる場合には、A社とB社は、それぞれ互いの秘密情報管理にユーザ認証の安全性を依存させることをさけるために、それぞれに異なる秘密情報を保持する。その結果、異なるユーザ認証サーバを用いることが必要となる。このような場合に、ユーザ認証サーバと共有する秘密情報を携帯電話毎に内蔵することとすると、それぞれのシステムにアクセスする際に、アクセスするシステムに対応する秘密情報を持つ携帯電話を選択して利用しなくてはならない。その結果、複数の形態電話を保有することとなり、コストが高く、利便性も悪くなる。しかし、本実施の形態のように、ICカードに秘密情報を格納するようにすれば、A社、B社のシステムを両方利用するユーザは、A社用のICカードとB社用のICカードを2つもち、それぞれのシステムにアクセスする際に、対応するICカードを携帯電話に挿入して表示されるワнтаイムパスワードを利用することができる。その結果、単一の携帯電話で、ユーザ認証を実行するユーザ認証サーバ毎に、異なる秘密情報を割り当てることが可能となり、コストは低く、利便性も向上する。

【0035】実施の形態4. 本実施の形態では、同期の元となる時刻情報を発信する時刻情報発信サーバにおいて、時刻の情報にデジタル署名を付与し、時刻携帯電話とユーザ認証サーバは現在時刻取得の際にその署名を検証する。図7は、実施の形態4における時刻情報発信サーバの構成図である。図8は、実施の形態4における現在時刻取得部の構成図である。図9は、実施の形態4における現在時刻取得処理のフローを示す図である。

【0036】時刻情報発信サーバ701では、タイマ702から現在時刻情報を取得すると（ステップS901）、秘密鍵情報格納部705に格納された公開鍵暗号方式の秘密鍵を用いて、署名生成部703により、時刻情報のデジタル署名を生成し、そのデジタル署名を時刻情報に付加する（ステップS902）。デジタル署名付き現在時刻情報は、現在時刻情報発信部704より、電

波により発信される（ステップS903）。

【0037】発信されたデジタル署名付き現在時刻情報は、携帯電話とユーザ認証サーバそれぞれの現在時刻情報受信部802で受信される。（ステップS904）その後、公開鍵格納部804に格納された公開鍵情報、つまり時刻情報発信サーバの秘密鍵情報に対応する公開鍵情報を用いて、署名検証部803により、デジタル署名の検証が行われる（S905）。検証に失敗した場合は、不正な時刻情報発信サーバにより発信された時刻情報であるか、途中で改ざんされた時刻情報であると判断し、受信した時刻情報を破棄する。検証に成功すれば、正しい時刻情報サーバから改ざんされずに送られてきた時刻情報と判断し、時刻情報を受け取る。受け取った時刻情報が、現在の携帯電話、認証サーバのタイマの示す時刻情報と、指定された範囲のずれを生じさせている場合には、携帯電話、認証サーバのタイマの時刻情報を、受信した時刻情報の値に修正する。但し、指定された時間以上ずれている場合には、携帯電話、認証サーバのタイマに異常があると判断し、エラーとする。

【0038】時刻情報発信サーバのデジタル署名付き時刻情報の発信間隔及び、受信側でのタイマ時刻修正を発生させる時間のずれの範囲については、任意の値に設定できる。例えば、時刻情報発信サーバのデジタル署名付き時刻情報の発信は、一日一回とし、受信側では、時刻情報とのずれが30秒以上5分以内のときは、受信した時刻情報に自らのタイマ情報を修正するように設定できる。

【0039】公開鍵暗号方式のアルゴリズムとしては、RSA、楕円暗号等アルゴリズムが使用可能である。

【0040】本実施の形態の効果について説明する。携帯電話、ユーザ認証サーバのタイマを、標準時刻に同期する際に、信頼できる発信元からの改ざんされていない時刻情報を用いることができるので、安全な時刻同期が可能となる。

【0041】

【発明の効果】本発明においては、同期する時刻と、共通の秘密情報に基づいて、ユーザIDに対応するワнтаイムパスワードを生成し、秘密情報の読み取りが不可である構成としているので、ワнтаイムパスワードの安全性を担保しつつ、秘密情報の管理を容易にすることができる。また、携帯電話でワнтаイムパスワードを生成するので、トークンを携帯する必要がなくなる。

【0042】ワнтаイムパスワード生成部は、ユーザIDを内部に保持し、入力するパラメータを時刻情報に限定しているので、携帯電話の分解によるワнтаイムパスワードの不正な生成を阻止することができる。

【0043】ワнтаイムパスワード生成部を、携帯電話に着脱可能なICカードにおいて実現するので、ユーザ認証サーバに対応するICカードを用いることにより、複数のユーザ認証サーバのサービスを簡単に享受するこ

とができる。

【0044】 デジタル認証された現在時刻により時刻を修正するので、常に適正な時刻情報に基づくワнтаイムパスワードが生成されるようになる。

【図面の簡単な説明】

【図1】 実施の形態1におけるユーザ認証システムの構成を示す図。

【図2】 実施の形態1におけるユーザ認証システムの概要を示す図。

【図3】 実施の形態1におけるユーザ認証システムの処理フローを示す図。

【図4】 ワнтаイムパスワード生成の詳細フローを示す図。

【図5】 実施の形態2におけるワнтаイムパスワード生成部の構成を示す図。

【図6】 実施の形態3における携帯電話とICカードの構成を示す図。

【図7】 実施の形態4における時刻情報発信サーバの構成図。

【図8】 実施の形態4における現在時刻取得部の構成図。

【図9】 実施の形態4における現在時刻取得処理のフローを示す図。

【図10】 トークンの外観を示す図。

【図11】 従来のワнтаイムパスワード認証システムの概要を示す図。

【図12】 秘密情報の管理状態を示す図。

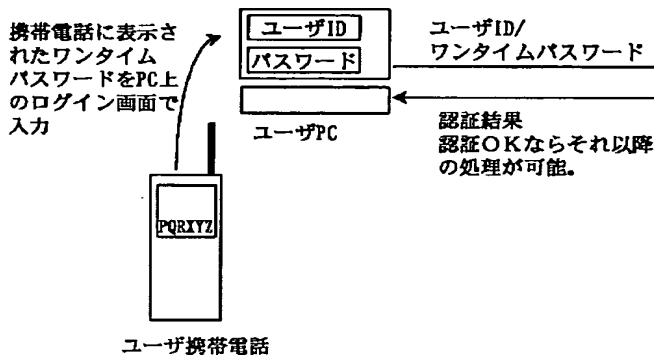
【図13】 従来技術におけるワнтаイムパスワード認証システムの構成を示す図。

【図14】 従来技術におけるワнтаイムパスワード認証システムの処理フローを示す図。

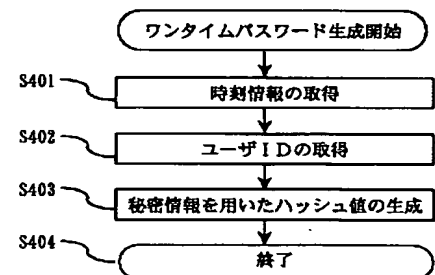
【符号の説明】

101 携帯電話、102 ユーザPC、103 ユーザ認証サーバ、104 伝送路、105 ワнтаイムパスワード表示部、106 現在時刻取得部、107 タイマ、108 ユーザID格納部、109 ワнтаイムパスワード生成部、110 時刻情報読み取り部、111 ユーザID情報読み取り部、112 秘密情報格納部、113 ハッシュ生成部、114 ワнтаイムパスワード格納部、115 ユーザID/パスワード入力部、116 ユーザID/パスワード送信部、117 認証結果受信部、118 現在時刻取得部、119 タイマ、120 ワнтаイムパスワード生成部、121 時刻情報読み取り部、122 ユーザID情報読み取り部、123 秘密情報格納部、124 ハッシュ生成部、125 ワнтаイムパスワード格納部、126 ワнтаイムパスワード検証部、127 ユーザID/ワнтаイムパスワード受信部、128 認証結果送信部、501 ワнтаイムパスワード生成部、502 時刻情報読み取り部、503 ユーザID格納部、504 ハッシュ生成部、505 ワнтаイムパスワード格納部、506 秘密情報格納部、601 携帯電話、602 ワнтаイムパスワード表示部、603 現在時刻取得部、604 タイマ、605 ICカード挿入部、606 ICカード、607 時刻情報読み取り部、608 ユーザID格納部、609 ハッシュ生成部、610 ワнтаイムパスワード格納部、611 秘密情報格納部、701 時刻情報発信サーバ、702 タイマ、703 署名生成部、704 現在時刻発信部、705 秘密鍵格納部、801 現在時刻取得部、802 現在時刻情報受信部、803 署名検証部、804 公開鍵格納部、805 現在時刻格納部。

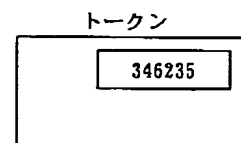
【図2】



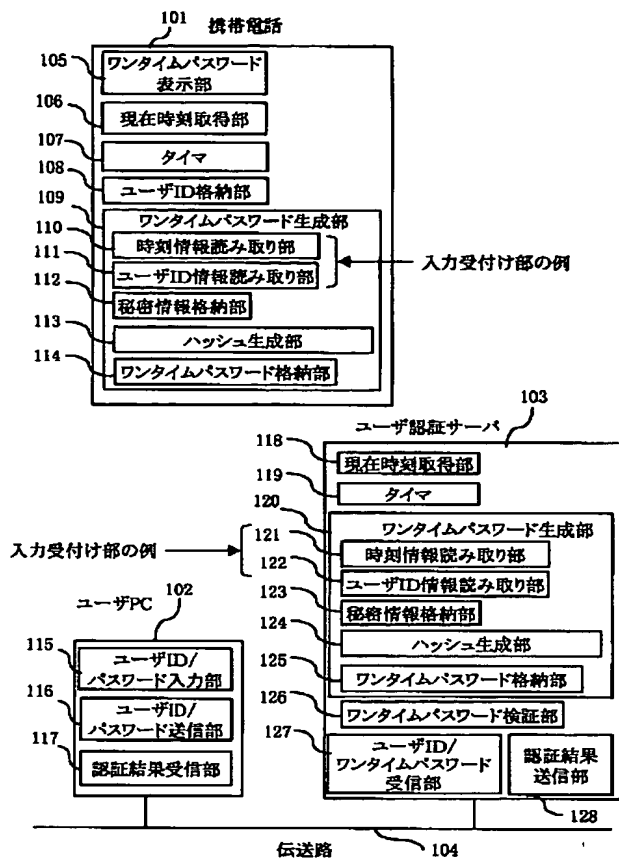
【図4】



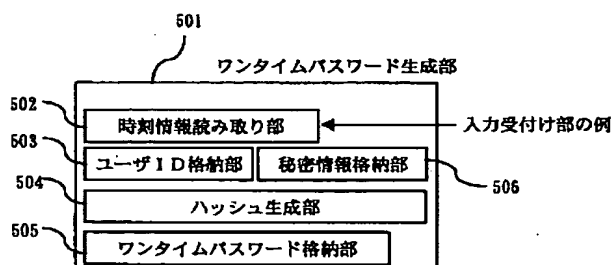
【図10】



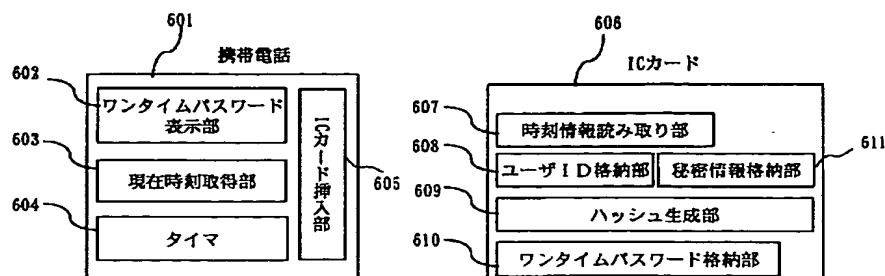
【図1】



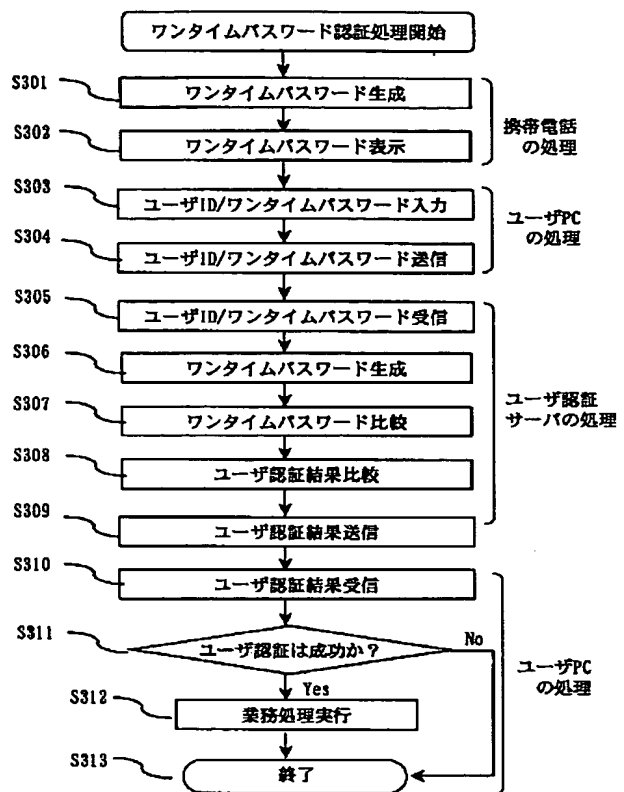
【図5】



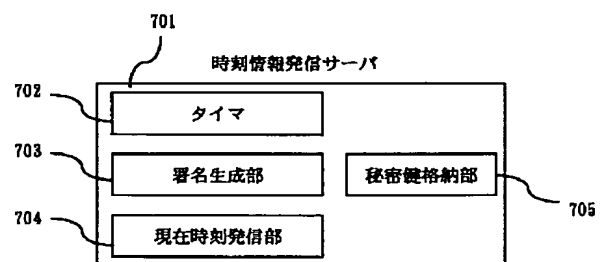
【図6】



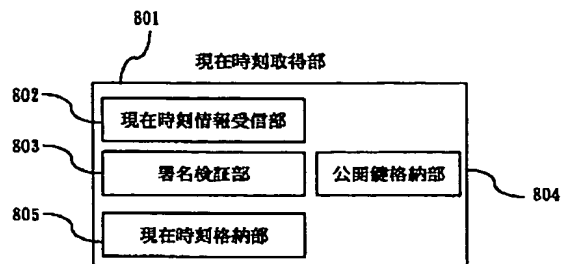
【図3】



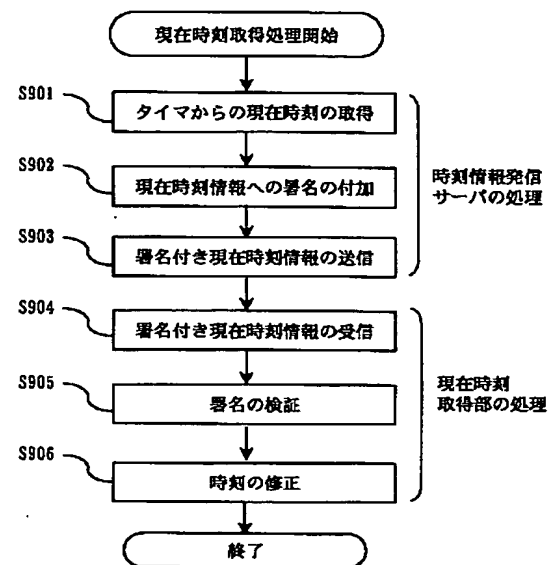
【図7】



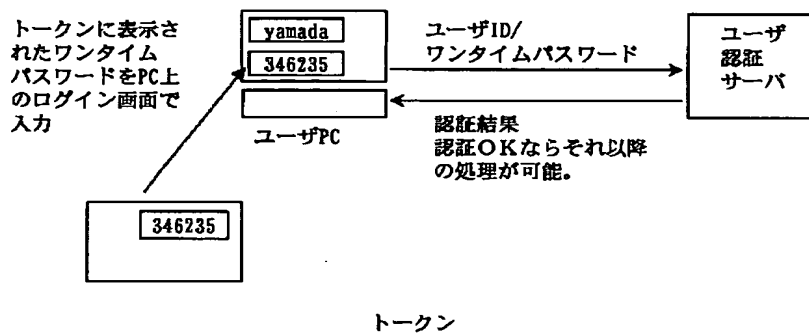
【図8】



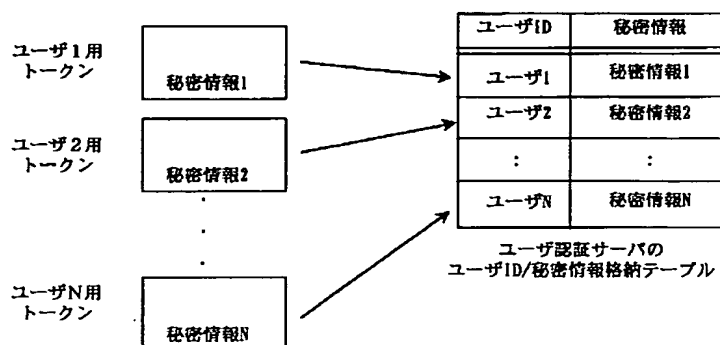
【図9】



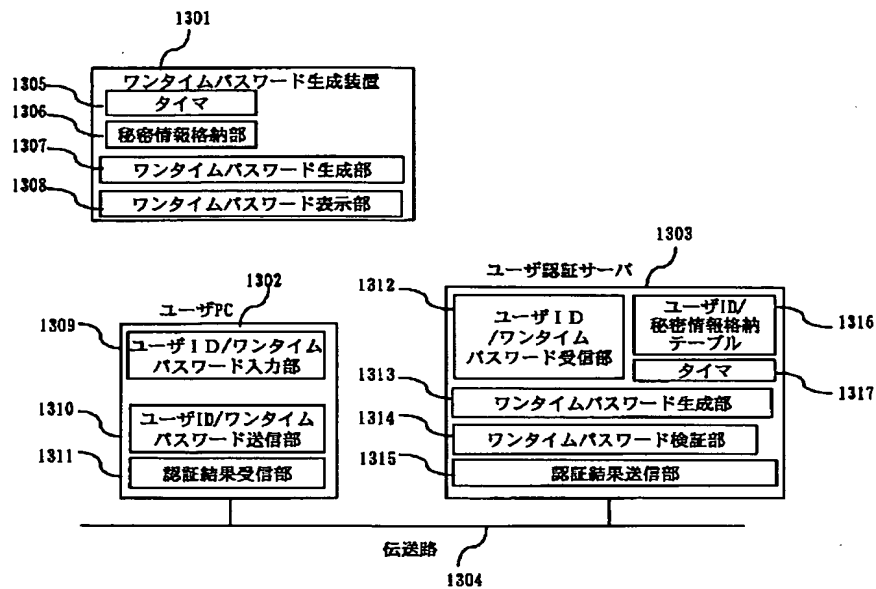
【図11】



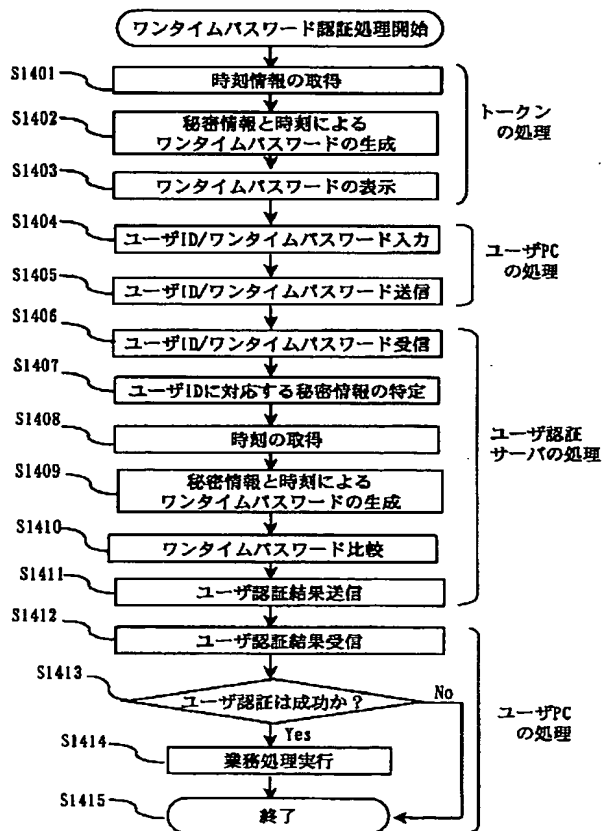
【図12】



【図13】



【図14】



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I
H 0 4 Q 7/04

ターマコード (参考)

B

Fターム(参考) 5B085 AE01 AE23 BG07
5J104 AA07 AA09 AA16 EA03 KA01
KA03 KA21 LA01 LA06 MA01
NA02 NA05 NA12 NA35 NA36
PA10
5K067 AA21 BB04 BB21 BB34 DD17
EE02 EE16 FF02 HH22 HH36
KK15